UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,595	12/31/2003	Tayib Sheriff	ITL.1079US (P18343)	8595

21906 7590 08/04/2006

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
FARROKH, HASHEM	
ART UNIT	PAPER NUMBER
2187	

DATE MAILED: 08/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/750,595	**Applicant(s)** SHERIFF ET AL.	
	Examiner Hashem Farrokh	**Art Unit** 2187	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9,11,13-18,22,24,26,29 and 31-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9,11,13-18,22 and 24* is/are allowed.

6)☒ Claim(s) *1-7,26,29 and 31-35* is/are rejected.

7)☒ Claim(s) *36* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This Office Action is in response to the Applicant's Remarks filed on May 15, 2006. The instant application having U.S. Patent No. 10/750,595 has a total of 25 claims pending in the application; claims 1-5, 7, 9, 11, 13, 15, 18, and 26 have been amended; claims 8, 10, 12, 19-21, 23, 25, 27-28, and 30 have been canceled; and claims 31-36 have been added.

The indicated allowability of claims 8 and 28 in the previous Office Action is withdrawn in view of the newly discovered reference(s). Rejections based on the newly cited reference(s) follow.

INFORMATION CONCERNING CLAIMS:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-7, 26, 29, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No. 2003/0140244 A1 to Dahan et al. (hereinafter Dahan) in view of U.S. Patent No. 5,895,487 to Boyd et al. (hereinafter Boyd).

1. In regard to claim 1 Dahan teaches:

“A system **(Fig. 1)** comprising: a process comprising multiple-mapped memory;” **(e.g., see paragraph 131 in page 11; table 4; Fig. 9).**

“a first set of memory mapped onto the multiple-mapped memory **(e.g, DATA 922 and 924 mapped to SECURE SRAM 902 and NON-SECURE SRAM 904; Fig. 9)**, a second set of memory mapped onto the multiple-mapped memory;” **(e.g., see paragraph 131 and Table 4 in page 11; CODE is mapped to SECURE ROM 900 and NON-SECURE ROM; Fig. 9)**. *Translation Lookaside Buffer (TLB) is used to perform memory mapping (e.g., Table 4 in page 11).*

“and an address overload circuit to selectively map the multiple-mapped memory to the first set of memory or to the second set of memory,” **(e.g., see paragraphs 50-51 in page 3; paragraphs 131-134 and Table 4 in page 11; Figs. 2 and 9).** *The memory management units (MMUs) (elements 210 and 212 in Fig. 2) include TLBs that performs the multiple memory mapping. However, Dahan does not expressly teach:* “the address overload circuit comprising an address multiplexer, an address translator coupled to the address multiplexer, and a data multiplexer.”

Boyd teaches: “the address overload circuit comprising an address multiplexer **(e.g., BANK ADR SELECTOR 1-4 in Fig. 9)**, an address translator coupled to the address multiplexer **(e.g., see column 13, lines 55-58… TLB in each processor nodes; Fig. 10)**, and a data multiplexer **(e.g., DATA SELECTOR 941-944 in Fig. 9)**” *for addressing and selecting data from ARRAY BANKS of memory.*

Disclosures by Dahan and Boyd are analogous because both references teach methods for mapping the address space to multiple memories.

At the time of invention it would have been obvious to a person of ordinary skill in art to modify the secure mode processors supporting MMU taught by Dahan to include the integrated address and data selectors (e.g., address overload circuit) *disclosed by Boyd.*

The motivation for using the address overload circuit as taught by column 12, lines 28-29 and 28-40 of Boyd is to fabricate an integrated address and data selectors with the array banks of memory on a single chip to simplify integration, layout and improve speed, density, etc.

Therefore, it would have been obvious to combine disclosures by Boyd with Dahan to obtain the invention as specified in the claim.

2. In regard to claim 2 Dahan teaches:

"wherein the second set of memory comprises instructions to execute a protected function." **(e.g., see abstract; element 416 in Fig. 4).** *For example ROM 311 shown in Fig. 4 include secure routine that* comprises instructions that are effective to execute a protected function.

3. In regard to claim 3 Dahan teaches:

"further comprising a transfer agent to receive parameters from the process and to assume control of execution of the process when the multiple-mapped memory is mapped to a protected set of memory."" **(e.g., see paragraph 45 in pages 2-3;**

element 302 in Fig. 3). *For example the ROM 310 includes the security agent and receives the security signal 302 or parameter shown in Fig. 3.*

4. *In regard to claim 4 Dahan teaches:*

"wherein the transfer agent is to call a protected function." **(e.g., see paragraph 83 in page 5; Fig. 5).**

5. *In regard to claim 5 Dahan teaches:*

"wherein the transfer agent is to call the protected function using parameters received from the process." **(e.g., see paragraph 45 in pages 2-3; element 302 in Fig. 3).**

6. *In regard to claim 6 Dahan teaches:*

"wherein the transfer agent is stored on nonvolatile memory." **(e.g., see element 416 in Fig. 4).** *For example ROM is a non-volatile memory.*

7. *In regard to claim 7 Dahan teaches:*

"wherein the transfer agent is to execute on internal memory." **(e.g., see paragraph 40 in page 2).** *The trusted or secure code or transfer agent is stored in ROM/SRAM. Both ROM and SRAM are internal or chip memories.*

8. *In regard to claim 26 Dahan teaches:*

"A system **(Fig. 1)** comprising: an integrated circuit device **(paragraph 169 in page 14; element 100 in Fig. 1)** comprising a processor **(element 102 in Fig. 1)**, internal random access memory (RAM) **(element 312 in Fig. 3)**, and internal read only memory (ROM);"

(element 311 in Fig. 3). *Fig. 3 is a block diagram of MPU 102 within the megacell 100, which is an integrated circuit and includes SRAM and ROM.*

"unprotected memory;" **(elements 311 and 313 in Fig. 3).** *Both SRAM and ROM include public or unprotected memories.*

"protected memory;" **(elements 310 and 312 in Fig. 3).** *Both SRAM and ROM include secure or protected memories.*

"a process to execute on the internal RAM **(paragraph 46 in page 3)**, the process comprising multiple-mapped memory **(Fig. 9)**, the multiple-mapped memory to be mapped to either the protected memory or the unprotected memory;" **(e.g., see claim 3).** *Dahan teaches that TLB has entries for both secure and unsecured mapping of virtual to physical address. Depending on mode of operation (e.g. Fig. 5) one of the translation or mapping to secure or unsecured inherently is selected.*

"a trust co-processor to determine whether the multiple-mapped memory is to be mapped to the unprotected memory or is to be mapped to the protected memory;" **(e.g., see paragraph 47 in page 3; element 150 in Fig. 1).** *For example Security State Machine (SSM) represent the co-processor stated in the claim.*

"a wireless interface coupled to the processor;" **(e.g., see paragraph 166 in page 14; element 18 in Fig. 12).**

"and an antenna coupled to the wireless interface." **(e.g., see paragraph 166 in page 14; element 18 in Fig. 12).** *Dahan teaches the wireless for use in communicating with* *other users of wireless network. Therefore, the wireless link disclosed inherently must be coupled to an antenna.*

"a circuit coupled to the trust co-processor **(e.g., SSM 150 in Fig. 1)** to map the multiple mapped memory to the protected memory," **(e.g., see paragraph 47 in page 3; paragraph 128 in page 10; element 150 in Fig. 1; Table 4 in page 11)**. *However, Dahan does not expressly teach:* "the circuit comprising an address multiplexer, an address translator coupled to the address multiplexer, and a data multiplexer."

Boyd teaches: "the comprising an address multiplexer **(e.g., BANK ADR SELECTOR 1-4 in Fig. 9)**, an address translator coupled to the address multiplexer **(e.g., see column 13, lines 55-58... TLB in each processor nodes; Fig. 10)**, and a data multiplexer **(e.g., DATA SELECTOR 941-944 in Fig. 9)**". *The motivation for combination is based on the same rational given for rejection of claim 1.*

9. *In regard to claim 29 Dahan teaches:*

"further comprising a transfer agent to receive parameters from a trusted process **(e.g., see paragraph 45 in pages 2-3; element 302 in Fig. 3)**, call a protected function using the parameters, and cause the protected function to execute."

10. *In regard to claim Boyd teaches:*

"a memory controller including circuit." **(e.g., see Fig. 9; DIRECTORY+ CONTROLS 1221-1224 IN Fig. 12).**

Claims 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,854,039 B1 to Strongin et al. (hereinafter Strongin) in view of U.S. Patent Publication No. 2002/0095545 A1 to Dalvi et al. (hereinafter Dalvi).

11. In regard to claim 32 Strongin teaches:

"An apparatus **(e.g., Fig. 4)** comprising:"

"an address selector **(e.g., Selection Logic 704 in Fig. 7)** to receive an address **(e.g., Linear Address from Segmentation Unit 700; Fig. 7)** and a translated address **(e.g., Address from Paging Unit 702; Fig. 7)**, the address selector to provide an output mapped to a respective one of a protected storage and unprotected storage;" **(e.g., see column 9, lines 35-50; column 10, lines 14-31; Column 13-14, Table).** *For example Strongin teaches that the linear address is translated or mapped to protected or unprotected pages. However, Strongin does not expressly teach:* "a data selector to receive data from the protected storage and unprotected storage."

Dalvi teaches: "a data selector to receive data from the protected storage **(e.g., element 214 in Fig. 3)** and unprotected storage." **(e.g., see paragraph 27 in page 2; paragraph 44 and 47 in page 4; claim 14 in page 8; Output MUX 202 and elements 214 and 212 in Fig. 3)** *for receiving and selecting data from protected or unprotected memory.*

Disclosures by Strongin and Dalvi are analogous because both references teach methods for memory management.

At the time of invention it would have been obvious to a person of ordinary skill in art to modify the memory management system and method taught by Strongin to include the programming protection taught by Dalvi.

The motivation for using the protection method as taught by paragraph 27, page 2 of Dalvi is to optimize the memory to processor interface.

Therefore, it would have been obvious to combine disclosures by Dalvi with Strongin to obtain the invention as specified in the claim.

12. In regard to claim 33 Strongin teaches:

"an address translator coupled to the address selector to generate the translated address." **(e.g., column 10, lines 66-67 to column 11, lines 1-3; element 702 and 704 in Fig. 7).** *For example paging unit 702 include Translation Lookaside Buffer (TLB) used to translate the linear addresses to physical addresses.*

13. In regard to claim 34 Strongin teaches:

"wherein the address selector is to map the output to the protected storage if a process is trusted." **(e.g., column 9, lines 65-67; claim 9 in page 19).** *For example in the protection mode the operation is protected or the process is trusted.*

Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Strongin in view of Dalvi as applied to claim 34 above, and further in view of Dahan.

14. In regard to claim 35 the combined teachings of Strongin and Boyd teach all limitations included in claim 34 but does not exclusively teach: "a trust coprocessor to determine if the process is trusted."

Dahan teaches*:* "a trust coprocessor **(e.g., SSM 150 IN Fig. 1)** to determine if the process is trusted." **(e.g., see paragraph 75 in page 5; Fig. 5)** *for determining if a requested service is a secure (e.g., trusted) operation).*

Disclosures by Strongin, Dalvi, and Dahan are analogous because all references related memory management.

At the time of invention it would have been obvious to a person of ordinary skill in art to modify the memory management system and method taught by Strongin to include the programming protection taught by Dalvi. Furthermore, to include secure method taught by Dahan.

The motivation for using security method as taught by paragraph 9, page 1 of Dahan is to improve security of operating system. Furthermore, the motivation for using the protection method as taught by paragraph 27, page 2 of Dalvi is to optimize the memory to processor interface.

Therefore, it would have been obvious to combine disclosures by Dahan with Dalvi and Strongin *to obtain the invention as specified in the claim.*

<u>ALLOWABLE SUBJECT MATTER</u>

Claims 9, 11, 13-18, 22, and 24 are allowed.

Claims 36 is objected to as being dependent upon rejected based claims, but would be allowable if rewritten in correct and independent form including all of the limitations of the base claim and any intervening claims.

1. The primary reason for allowance of claims 9, 11, and 13-17 are allowed in instant application is the combination with the inclusion of the following limitations: **if the process is determined to be a trusted process, mapping the multiple-mapped memory to protected memory, copying the transfer agent to a second memory, transferring parameters from the process to the transfer agent, and controlling execution of the process with transfer agent.**

"and (c) a data multiplexer."

2. The primary reason for allowance of claims 18, 22, and 24 in instant application is the combination with the inclusion of the following limitations: **if the process is a trusted process, transfer, at least temporarily, control of the process to a transfer agent and transfer process parameters to transfer agent; identify and execute a protected function; and copy the transfer agent from nonvolatile memory to volatile memory in the course of executing multiple-mapped memory.**

3. The primary reason for allowance of claim 36 in instant application is the combination with the inclusion of the following limitations: **the address selector and the data selector are to be controlled by a control signal from the wherein trust coprocessor.**

*: **IMPORTANT NOTE** :*

*I f the applicant should choose to rewrite the independent claims to include the limitations recited in either one of the claims, the applicant is encouraged to **amend the title of the invention** such that it is descriptive of the invention as claimed as required be sec. **606.01** of the **MPEP**. Furthermore, the **summary of invention** and the **abstract** should be amended to bring them into harmony with the allowed claims as required by paragraph 2 of **sec. 1302.01** of the **MPEP**.*

*As allowable subject matter has been indicated, applicant's response must either comply with all formal requirements or specifically traverse each requirement not compiled with. See **37 C.F.R. § 1.111(b)** and **§ 707.07(a) of the M.P.E.P.***

Response to Applicant's Remarks

In view of newly discovered references the indicated allowability of some the subject matter indicated in previous Office Action has been withdrawn. The Examiner apologizes if this would cause any inconveniences.

Conclusion

The prior art made of record and not relied upon are as follows:

1. *U. S. Patent No. 6,606,707 B1 to Hirota et al. Semiconductor memory card.*

2. *U. S. Patent Publication No. 2005/0055524 A1 to* Gulick *et al. describes Computer system employing a trusted execution environment including a memory controller configured to clear memory.*

3. *U. S. Patent No. 6,775,750 B2 to* Krueger *describes System protection map.*

Any inquiry concerning this communication should be directed to Hashem Farrokh whose telephone number is (571) 272-4193. The examiner can normally be reached Monday-Friday from ***8:00 AM to 5:00 PM.***

If attempt to reach the above noted Examiner by telephone are unsuccessful, the examiner's supervisor, Mr. Donald A Sparks, can be reached on (571) 272-4201. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published application may be obtained from either private PAIR or Public PAIR. Status information for unpublished application is available through Private PAIR only. For more information about PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBS) at 866-217-9197 (toll-free).

HF

2006-07-31

Brian R Peugh
Primary Examiner